IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Applicant:		§	Art Unit:	2431
	Mark D. Yarvis	§		
		§	Examiner:	Kaveh Abrishamkar
Serial No.:	10/812,651	§		
		§	Conf. No.:	3419
Filed:	March 29, 2004	§		
		§	Docket:	ITL.1954US
For:	Radio Frequency Identification	§		P18388
	Tag Lock and Key	§		
		§	Assignee:	Intel Corporation

Mail Stop **Appeal Brief-Patents**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Date of Deposit: May 28, 2010
I hereby certify that this correspondence is being electronically transmitted on the date indicated above.

Cynthia L. Hayden

Cynthia L. Hayden

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party in interest is the assignee Intel Corporation.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 1-8 (Rejected).

Claims 9-13 (Canceled).

Claim 14 (Rejected).

Claim 15 (Canceled).

Claims 16-17 (Rejected).

Claim 18 (Canceled).

Claims 19-20 (Rejected).

Claims 21-25 (Canceled).

Claim 26 (Rejected).

Claim 27 (Canceled).

Claims 28-29 (Rejected).

Claim 30 (Canceled).

Claims 31-32 (Rejected).

Claims 33-36 (Canceled).

Claims 1-8, 14, 16, 17, 19, 20, 26, 28, 29, 31, and 32 are rejected and are the subject of this appeal brief.

STATUS OF AMENDMENTS

All amendments have been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

In the following discussion, the independent claims are read on one of many possible embodiments without limiting the claims:

1. An apparatus, comprising:

a detector (Fig. 2, 200) to determine whether a first radio frequency identification tag (Fig. 1, 114) read by a reader (Fig. 1, 118) that reads radio frequency identification tags is a match with a second radio frequency identification tag read by said reader (Specification at page 7, lines 1-6).

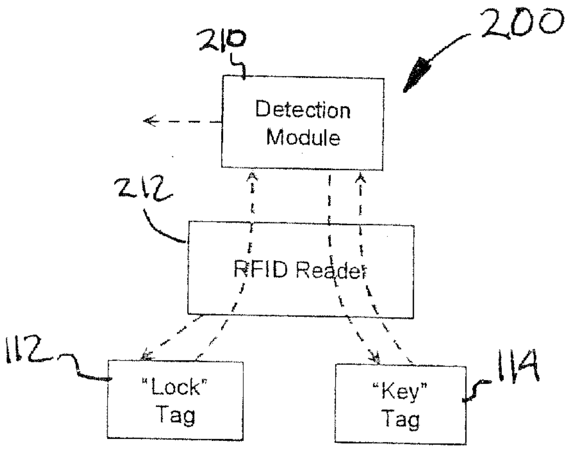

FIG. 2

14. A method, comprising:

generating a nonce (Fig. 3, 310) (Specification at page 8, lines 12-14);

encrypting the nonce (Fig. 3, 312) using a cryptography key received from a first radio frequency identification tag to result in an encrypted nonce (Specification at page 8, lines 12-14);

sending the encrypted nonce to a second radio frequency identification tag (Fig. 3, 113) that decrypts the encrypted nonce to result in a decrypted nonce (Specification at page 8, lines 16-18);

receiving the nonce from the second radio frequency identification tag (Specification at page 8, lines 18-20);

comparing the nonce (Fig. 3, 320) generated by said generating to the decrypted nonce (Specification at page 8, lines 22-24); and

determining (Fig. 3, 320), as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag (Specification at page 8, lines 22-24).

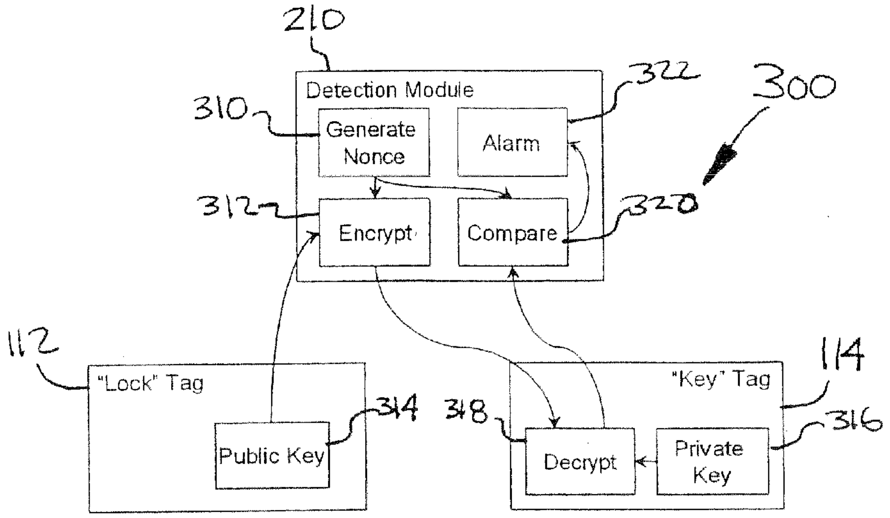

FIG.3

17. A method, comprising:

generating a series of nonces (Fig. 5, 510) (Specification at page 10, lines 8-14);

sending (Fig. 5, n_i) the series of nonces to a first radio frequency identification tag and a second radio frequency identification tag (Specification at page 9, lines 19-20);

receiving encrypted versions of the series of nonces (Fig. 5, E_k) from the first and second radio frequency identification tags (Specification at page 9, lines 22-24);

comparing the encrypted versions of the series of nonces (Fig. 5, 524) received from the first radio frequency identification tag with the encrypted versions of the series of nonces received from the second radio frequency identification tag (Specification at page 9, lines 25-27); and

determining (Fig. 3, 320), as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag (Specification at page 9, lines 25-27).

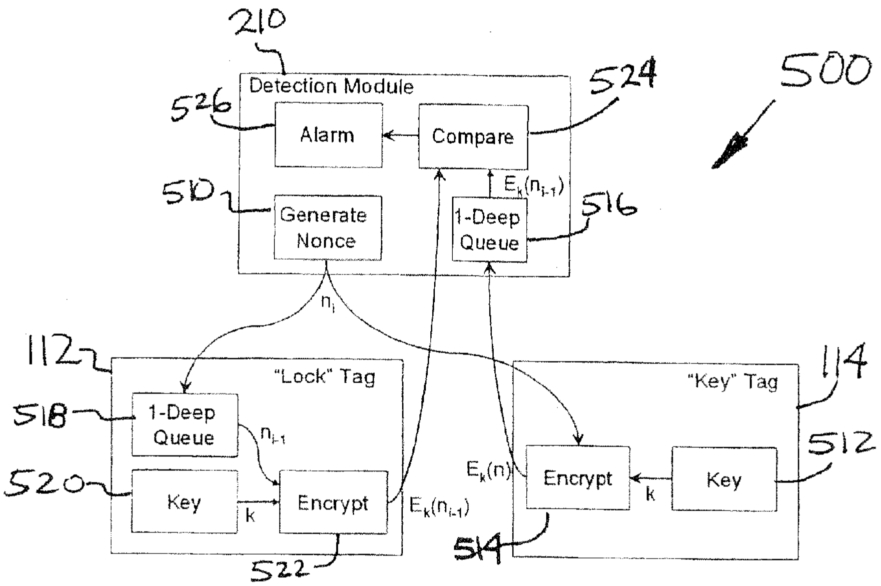

FIG.5

26. An article comprising a storage medium having stored thereon instructions that, when executed by a computing platform, result in verification of association of at least two or more radio frequency identification tags by:

generating a nonce (Fig. 3, 310) (Specification at page 8, lines 12-14);

encrypting the nonce (Fig. 3, 312) using a cryptography key received from a first radio frequency identification tag to result in an encrypted nonce (Specification at page 8, lines 12-14);

sending the encrypted nonce to a second radio frequency identification tag (Fig. 3, 113) that decrypts the encrypted nonce to result in a decrypted nonce (Specification at page 8, lines 16-18);

receiving the nonce from the second radio frequency identification tag (Specification at page 8, lines 18-20);

comparing the nonce (Fig. 3, 320) generated by said generating to the decrypted nonce (Specification at page 8, lines 22-24); and

determining (Fig. 3, 320), as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag (Specification at page 8, lines 22-24).

29. An article comprising a storage medium having stored thereon instructions that, when executed by a computing platform, result in verification of association of at least two or more radio frequency identification tags by:

generating a series of nonces (Fig. 5, 510) (Specification at page 10, lines 8-14);

sending (Fig. 5, n_i) the series of nonces to a first radio frequency identification tag and a second radio frequency identification tag (Specification at page 9, lines 19-20);

receiving encrypted versions of the series of nonces (Fig. 5, E_k) from the first and second radio frequency identification tags (Specification at page 9, lines 22-24);

comparing the encrypted versions of the series of nonces (Fig. 5, 524) received from the first radio frequency identification tag with the encrypted versions of the series of nonces received from the second radio frequency identification tag (Specification at page 9, lines 25-27); and determining (Fig. 3, 320), as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag (Specification at page 9, lines 25-27).

At this point, no issue has been raised that would suggest that the words in the claims have any meaning other than their ordinary meanings. Nothing in this section should be taken as an indication that any claim term has a meaning other than its ordinary meaning.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether claims 1-3 are anticipated under 35 U.S.C. § 102(e) by Reynolds.

B. Whether claims 4-8, 14, 16, 17, 19, 20, 26, 28, 29, 31, and 32 are unpatentable under 35 U.S.C. § 103(a) over Reynolds in view of Lapstun.

ARGUMENT

A. Are claims 1-3 anticipated under 35 U.S.C. § 102(e) by Reynolds?

Reynolds is all about making sure that the RFID tag that it is being read is associated with a particular object. The way Reynolds works is he confirms that the object that he is reading the RFID tag on is the object he thinks it is by reading a visual indication, such as a barcode. The cited paragraphs 81 and 82 explain this operation.

It would make no sense for Reynolds to use two bar tags and to compare the readings. That is because reading either or both bar tags still gives him no confirmation that the object that he is looking at is the one whose RFID tag was read.

For example, if you think about a number of objects in a room and you are getting an RFID tag reading, but there is a bunch of objects physically close together so you do not know which RFID tag is the one you are reading. So you simply see a visual marker, like a barcode, read that and then see if the barcode matches the RFID tag. Reading another RFID tag to compare to the first RFID tag would leave you no better information.

Thus, Reynolds simply does not meet the claimed limitations and the rejection should be reversed.

B. Are claims 4-8, 14, 16, 17, 19, 20, 26, 28, 29, 31, and 32 unpatentable under 35 U.S.C. § 103(a) over Reynolds in view of Lapstun?

For the reasons set forth above, these rejections should also be reversed.

*   *   *

Applicant respectfully requests that each of the final rejections be reversed and that the claims subject to this Appeal be allowed to issue.

Respectfully submitted,

Date: May 28, 2010

/Timothy N. Trop/
Timothy N. Trop, Reg. No. 28,994
TROP, PRUNER & HU, P.C.
1616 South Voss Road, Suite 750
Houston, TX 77057-2631
713/468-8880 [Phone]
713/468-8883 [Fax]

Attorneys for Intel Corporation

CLAIMS APPENDIX

The claims on appeal are:

1. An apparatus, comprising:

a detector to determine whether a first radio frequency identification tag read by a reader that reads radio frequency identification tags is a match with a second radio frequency identification tag read by said reader.

2. An apparatus as claimed in claim 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag.

3. An apparatus as claimed in claim 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector authenticates the lock tag when said detector detects the lock tag and the key tag being within a predetermined distance of said detector.

4. An apparatus as claimed in 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector includes a nonce generator to generate a nonce, an encryptor to encrypt a nonce using a public cryptography key received from the lock tag to provide an encrypted nonce to the key tag, and a comparator to compare a nonce generated by the nonce generator with a decrypted version of the encrypted nonce that was decrypted using a private cryptography key of the key tag.

5. An apparatus as claimed in claim 1, wherein one of the first and second radio frequency identification tags is a lock tag, and another of the first and second radio frequency identification tags is a key tag, and wherein said detector includes a nonce generator to generate a nonce, and a comparator to compare an encrypted version of the nonce encrypted using a

cryptography key of the lock tag with an encrypted version of the nonce encrypted using a cryptography key of the key tag.

6. An apparatus as claimed in claim 5, wherein the cryptography key of the lock tag is the same as the cryptography key of the key tag.

7. An apparatus as claimed in claim 5, wherein the nonce generator generates a series of nonces, wherein the lock tag delays encryption of the nonce with respect to encryption of the nonce by the key tag, and wherein said detector further comprises a delay to delay the encrypted version of the nonce encrypted by the key tag.

8. An apparatus as claimed in claim 1, wherein said detector determines whether the first radio frequency identification tag is a match with the second radio frequency identification tag or a third or more radio frequency identification tags.

14. A method, comprising:

generating a nonce;

encrypting the nonce using a cryptography key received from a first radio frequency identification tag to result in an encrypted nonce;

sending the encrypted nonce to a second radio frequency identification tag that decrypts the encrypted nonce to result in a decrypted nonce;

receiving the nonce from the second radio frequency identification tag;

comparing the nonce generated by said generating to the decrypted nonce; and

determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag.

16. A method as claimed in claim 14, wherein the cryptography key received from the first radio frequency identification tag is a public key, and wherein the second radio frequency identification tag decrypts the encrypted nonce using a private key associated with the public key.

17. A method, comprising:

generating a series of nonces;

sending the series of nonces to a first radio frequency identification tag and a second radio frequency identification tag;

receiving encrypted versions of the series of nonces from the first and second radio frequency identification tags;

comparing the encrypted versions of the series of nonces received from the first radio frequency identification tag with the encrypted versions of the series of nonces received from the second radio frequency identification tag; and

determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag.

19. A method as claimed in claim 17, wherein the first and second radio frequency identification tags encrypt the series of nonces using the same cryptography key.

20. A method as claimed in claim 17, wherein the first radio frequency radio identification tag delays the series of nonces with respect to the second radio frequency identification tag, and further comprising delaying the encrypted versions of the series of nonces received from the second radio frequency identification tag prior to said comparing.

26. An article comprising a storage medium having stored thereon instructions that, when executed by a computing platform, result in verification of association of at least two or more radio frequency identification tags by:

generating a nonce;

encrypting the nonce using a cryptography key received from a first radio frequency identification tag to result in an encrypted nonce;

sending the encrypted nonce to a second radio frequency identification tag that decrypts the encrypted nonce to result in a decrypted nonce;

receiving the nonce from the second radio frequency identification tag;

comparing the nonce generated by said generating to the decrypted nonce; and determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag.

28. An article as claimed in claim 26, wherein the cryptography key received from the first radio frequency identification tag is a public key, and wherein the second radio frequency identification tag decrypts the encrypted nonce using a private key associated with the public key.

29. An article comprising a storage medium having stored thereon instructions that, when executed by a computing platform, result in verification of association of at least two or more radio frequency identification tags by:

generating a series of nonces;

sending the series of nonces to a first radio frequency identification tag and a second radio frequency identification tag;

receiving encrypted versions of the series of nonces from the first and second radio frequency identification tags;

comparing the encrypted versions of the series of nonces received from the first radio frequency identification tag with the encrypted versions of the series of nonces received from the second radio frequency identification tag; and

determining, as a result of said comparing, whether the first radio frequency identification tag is associated with said second radio frequency identification tag.

31. An article as claimed in claim 29, wherein the first and second radio frequency identification tags encrypt the series of nonces using the same cryptography key.

32. An article as claimed in claim 29, wherein the first radio frequency radio identification tag delays the series of nonces with respect to the second radio frequency identification tag, and wherein the instructions, when executed, further result in verification of association of at least two or more radio frequency identification tags by comprising delaying the encrypted versions of the series of nonces received from the second radio frequency identification tag prior to said comparing.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None